The DevOps Company

Microsoft Partner

# MS-500T00
# Microsoft 365 Security Administration

## Sobre este curso.

En este curso aprenderá cómo asegurar el acceso de los usuarios a los recursos de su organización. El curso cubre la protección de contraseña de usuario, la autenticación multifactor, cómo habilitar la Protección de identidad de Azure, cómo configurar y usar Azure AD Connect, y le presenta el acceso condicional en Microsoft 365. Aprenderá sobre las tecnologías de protección contra amenazas que ayudan a proteger su entorno Microsoft 365. Específicamente, aprenderá acerca de los vectores de amenazas y las soluciones de seguridad de Microsoft para mitigar las amenazas. Aprenderá sobre Secure Score, la protección de Exchange Online, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection y la gestión de amenazas. En este curso aprenderá sobre las tecnologías de protección de la información que ayudan a proteger su entorno Microsoft 365. Este curso analiza el contenido administrado por los derechos de información, el cifrado de mensajes, así como las etiquetas, políticas y reglas que admiten la prevención de pérdida de datos y la protección de la información. Finalmente, en este curso aprenderá sobre el archivado y la retención en Microsoft 365, así como sobre el gobierno de datos y cómo realizar búsquedas e investigaciones de contenido. Este curso cubre las políticas y etiquetas de retención de datos, la administración de registros en el lugar para SharePoint, la retención de correo electrónico y cómo realizar búsquedas de contenido que admitan investigaciones de descubrimiento electrónico.

## Duración.

4 Días.

## Perfil del público.

El Microsoft 365 Security Administrator colabora con el Microsoft 365 Enterprise Administrator, las partes interesadas de negocios y otros administradores de carga de trabajo para planificar e implementar estrategias de seguridad y garantiza que las soluciones cumplan con las directivas y regulaciones de la organización. Este rol asegura proactivamente los entornos empresariales de Microsoft 365. Las responsabilidades incluyen responder a amenazas, implementar, administrar y monitorear soluciones de seguridad y cumplimiento para el entorno de Microsoft 365. Responden a incidentes, investigaciones y aplicación de la gobernanza de datos. El administrador de seguridad de Microsoft 365 está familiarizado con las cargas de trabajo de Microsoft 365 y los entornos híbridos. Este rol tiene fuertes habilidades y experiencia con protección de identidad, protección de información, protección contra amenazas, gestión de seguridad y gobierno de datos.

## Requisitos previos.

Los estudiantes que comiencen este curso ya deben contar con:

- Comprensión conceptual básica de Microsoft Azure.
- Experiencia con dispositivos Windows 10.
- Experiencia con Office 365.
- Conocimientos básicos de autorización y autenticación.
- Conocimientos básicos de redes informáticas.
- Conocimiento práctico de la administración de dispositivos móviles.

## Examen.

MS-500: Microsoft 365 Security Administration.

## Temario.

### Módulo 1: Crear, configurar y administrar identidades.

El acceso a las cargas de trabajo basadas en la nube debe controlarse de forma centralizada al proporcionar una identidad definitiva para cada usuario y recurso. Puede asegurarse de que los empleados y los proveedores tengan el acceso suficiente para realizar su trabajo.

- Crear, configurar y administrar usuarios.
- Creación, configuración y administración de grupos.
- Configuración y administración del registro de dispositivos.
- Administrar licencias.
- Creación de atributos de seguridad personalizados.
- Exploración de la creación automática de usuarios.

**Ejercicios:**

- Asignar licencias a usuarios.
- Restaurar o quitar usuarios eliminados.
- Agregar grupos en Azure Active Directory.
- Cambiar las asignaciones de licencias de grupo.
- Cambiar las asignaciones de licencias de usuario.

**Al término de este módulo, podrá:**

- Crear, configurar y administrar usuarios.
- Crear, configurar y administrar grupos.
- Administrar licencias.
- Explicación de los atributos de seguridad personalizados y el aprovisionamiento automático de usuarios.

### Módulo 2: Explora la sincronización de identidades.

Este módulo examina la sincronización de identidades utilizando Azure AD Connect y explora las opciones de autenticación y aprovisionamiento que se pueden utilizar y el funcionamiento interno de la sincronización de directorios.

- Examinar las opciones de autenticación en Microsoft 365.
- Examinar las opciones de aprovisionamiento en Microsoft 365.
- Explorar la sincronización de directorios.
- Explora Azure AD Connect.

**Al final de este módulo, podrás:**

- Describir las opciones de autenticación y aprovisionamiento de Microsoft 365.
- Explicar la sincronización de directorios.
- Explique cómo Azure AD Connect permite la coexistencia entre su entorno local de Active Directory y Microsoft 365.

### Módulo 3: Implementación y administración de una identidad híbrida.

Crear una solución de identidad híbrida para usar su instancia local de Active Directory puede ser todo un desafío. Consulte cómo puede implementar una solución de identidad híbrida segura.

- Planificación, diseño e implementación de Azure Active Directory Connect.
- Implementación y administración de la sincronización de hash de contraseña (PHS).
- Implementación y administración de la autenticación de tránsito (PTA).
- Implementación y administración de la federación.
- Solución de errores de sincronización.
- Implementación de Azure Active Directory Connect Health.
- Administración de Azure Active Directory Connect Health.

**Demostración:**

- Administración de la autenticación transferida y el inicio de sesión único (SSO) de conexión directa.

**Al final de este módulo, podrá hacer lo siguiente:**

- Planeación, diseño e implementación de Azure Active Directory Connect (AADC)
- Administración de Azure Active Directory Connect (AADC)
- Administración de la sincronización de hash de contraseña (PHS)
- Administración de la autenticación de tránsito (PTA)
- Administración del inicio de sesión único de conexión directa (SSO de conexión directa)
- Administración de la federación excluyendo las implementaciones manuales de ADFS
- Solución de errores de sincronización
- Implementación y administración de Azure Active Directory Connect Health

## Módulo 4: Implementación y administración de identidades externas.

La posibilidad de invitar a usuarios externos a usar los recursos de Azure de la empresa es una gran ventaja, pero debe hacerlo de manera segura. Explore cómo habilitar la colaboración externa segura.

- Descripción del acceso de invitado y las cuentas de negocio a negocio.
- Administración de la colaboración externa.
- Invitación a usuarios externos, de forma individual y masiva.
- Implementación de controles de acceso entre inquilinos.
- Configuración de proveedores de identidades.
- Implementación y administración de Entra Verified ID.

**Demostración:**

- Administración de los usuarios invitados en Azure Active Directory.
- Administrar cuentas de usuario externas en Azure Active Directory.
- Administración de usuarios externos en cargas de trabajo de Microsoft 365.

**Ejercicios:**

- Configurar la colaboración externa.
- Agregar usuarios invitados a un directorio.
- Invitar a usuarios invitados de forma masiva.
- Explorar los grupos dinámicos.

**Al final de este módulo, podrá:**

- Administrar la configuración de colaboración externa en Azure Active Directory.
- Invitar a usuarios externos (de forma individual o masiva).
- Administrar cuentas de usuario externas en Azure Active Directory.
- Configurar proveedores de identidades (sociales y SAML/ WS-Fed).

## Módulo 5: Administrar el acceso seguro de los usuarios en Microsoft 365.

Este módulo examina varias tareas relacionadas con contraseñas para cuentas de usuario y administrador, como la creación y configuración de políticas de contraseñas, la configuración de la gestión de contraseñas de autoservicio, la configuración de la autenticación multifactorial y la implementación de paquetes de derechos y políticas de acceso condicional.

- Administrar contraseñas de usuario.
- Habilitar la autenticación de paso.
- Habilitar la autenticación multifactor.
- Explora la gestión de contraseñas de autoservicio.
- Implementar Azure AD Smart Lockout.
- Implementar paquetes de derechos en Azure AD Identity Governance.
- Implementar políticas de acceso condicional.
- Crear y ejecutar una revisión de acceso.
- Investigar los problemas de autenticación utilizando los registros de inicio de sesión.

**Al final de este módulo, podrás:**

- Administrar contraseñas de usuario
- Describir la autenticación de paso
- Habilitar la autenticación multifactor
- Describir la gestión de contraseñas de autoservicio
- Implementar Azure AD Smart Lockout
- Implementar paquetes de derechos en Azure AD Identity Governance
- Implementar políticas de acceso condicional
- Crear y realizar una revisión de acceso

## Módulo 6: Administrar la autenticación de usuarios.

Hay varias opciones para la autenticación en Azure AD. Aprenda a implementar y administrar las autenticaciones correctas para los usuarios en función de las necesidades empresariales.

- Administrar FIDO2 y métodos de método de autenticación sin contraseña.
- Exploración de la aplicación Authenticator y tokens de OATH.
- Implementar una solución de autenticación basada en Windows Hello para empresas.
- Implementación y administración de la protección de contraseñas.
- Configuración de umbrales de bloqueo inteligente
- Implementación de Kerberos y autenticación basada en certificados en Azure AD.
- Configuración de la autenticación de usuarios de Azure AD para máquinas virtuales.

**Ejercicios:**

- Configurar e implementar el autoservicio de restablecimiento de contraseña.
- Administración de los valores de bloqueo inteligente de Azure Active Directory.

**Al final de este módulo, podrá:**

- Administrar métodos de autenticación (FIDO2/sin contraseña).
- Implementar una solución de autenticación basada en Windows Hello para empresas.
- Configurar e implementar el autoservicio de restablecimiento de contraseña.
- Implementación y administración de la protección de contraseñas.
- Implementación y administración de restricciones de inquilino.

## Módulo 7: Planificación, implementación y administración del acceso condicional.

El acceso condicional proporciona una gran granularidad de control sobre qué usuarios pueden realizar actividades concretas, acceder a recursos y garantizar que los datos y los sistemas sean seguros.

- Planificación de los valores predeterminados de seguridad.
- Planificación de directivas de acceso condicional.
- Implementación de controles y asignaciones de directivas de acceso condicional.
- Prueba de las directivas de acceso condicional y solución de problemas relacionados.
- Implementación de controles de aplicación.
- Implementación de la administración de sesiones.
- Implementación de la evaluación continua de acceso.

**Ejercicios:**

- Uso de los valores predeterminados de seguridad.
- Implementación de roles y asignaciones de directivas de acceso condicional.
- Configuración de los controles de sesión de autenticación.

**Al final de este módulo, podrá:**

- Planear e implementar los valores predeterminados de seguridad.
- Planear directivas de acceso condicional.
- Implementar controles y asignaciones de directivas de acceso condicional (destino, aplicaciones y condiciones).
- Probar las directivas de acceso condicional y solucionar los problemas relacionados.
- Implementar controles de aplicación.
- Implementar la administración de sesiones.
- Configurar umbrales de bloqueo inteligente.

## Módulo 8: Planificación e implementación de acceso con privilegios.

Es necesario asegurarse de que los roles administrativos están protegidos y administrados para aumentar la seguridad de la solución de Azure. Explore cómo usar PIM para proteger sus datos y recursos.

- Definición de una estrategia de acceso con privilegios para usuarios administrativos.
- Configurar Privileged Identity Management para recursos de Azure.
- Planificación y configuración de grupos de acceso con privilegios.
- Análisis del historial de auditoría e informes de Privileged Identity Management.
- Crear y administrar cuentas de acceso de emergencia.

**Ejercicios:**

- Configuración de Privileged Identity Management para los roles de Azure Active Directory.
- Asignación de roles de Azure Active Directory en Privileged Identity Management.
- Asignación de roles de recursos de Azure en Privileged Identity Management.

**Al final de este módulo, podrá:**

- Definir una estrategia de acceso con privilegios para usuarios administrativos (recursos, roles, aprobaciones y umbrales).
- Configuración de Privileged Identity Management para roles de Azure AD.
- Configurar Privileged Identity Management para recursos de Azure.
- Asignación de roles.
- Administrar solicitudes de PIM.
- Analizar el historial de auditorías y los informes de PIM.
- Crear y administrar cuentas de acceso de emergencia.

## Módulo 9: Planificación e implementación de la administración de derechos.

Cuando usuarios nuevos o usuarios externos se unen a su sitio, es necesario asignarles rápidamente acceso a las soluciones de Azure. Explore cómo autorizar a los usuarios para que accedan a su sitio y sus recursos.

- Definición de los paquetes de acceso.
- Configuración de la administración de derechos.
- Configuración y administración de organizaciones conectadas.
- Revisión de derechos por usuario.

**Ejercicios:**

- Creación y administración de un catálogo de recursos con derechos de Azure AD.
- Adición del informe de aceptación de los términos de uso.
- Administración del ciclo de vida de los usuarios externos con Azure AD Identity Governance.

**Al final de este módulo, podrá:**

- Definir catálogos.
- Revisar paquetes de acceso.
- Planear, implementar y administrar los derechos.
- Implementar y administrar las condiciones de uso.
- Administrar el ciclo de vida de los usuarios externos en la configuración de Azure AD Identity Governance.

## Módulo 10: Administración de Azure AD Identity Protection.

La protección de la identidad de un usuario mediante la supervisión de sus patrones de uso e inicio de sesión garantizará una solución de nube segura. Explore cómo diseñar e implementar Azure AD Identity Protection.

- Revisión de los conceptos básicos de Identity Protection.
- Implementación y administración de directivas de riesgo de usuario.
- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado.
- Implementación de la seguridad para las identidades de carga de trabajo.
- Explorar Microsoft Defender for Identity.

**Ejercicio:**

- Habilitación de una directiva de riesgo de inicio de sesión.
- Configuración de la directiva de registro de autenticación multifactor de Azure Active Directory.

**Al final de este módulo, podrá hacer lo siguiente:**

- Implementar y administrar directivas de riesgo de usuario, así como de inicio de sesión.
- Implementar y administrar una directiva de registro de autenticación multifactor.
- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado.

## Módulo 11: Protege contra amenazas con Microsoft Defender para Endpoint.

Descubra cómo Microsoft Defender for Endpoint puede ayudar a su organización a mantenerse segura.

- Introducción a Microsoft Defender para Endpoint.
- Practicar la administración de seguridad.
- Caza amenazas dentro de tu red.

**En este módulo, aprenderás a:**

- Defina las capacidades de Microsoft Defender para Endpoint.
- Comprende cómo cazar amenazas dentro de tu red.
- Explique cómo Microsoft Defender for Endpoint puede remediar los riesgos en su entorno.

## Módulo 12: Implementación del entorno de Microsoft Defender para punto de conexión.

Aprenda a implementar el entorno de Microsoft Defender para punto de conexión, incluidas la incorporación de dispositivos y la configuración de seguridad.

- Creación del entorno.
- Descripción de la compatibilidad y las características de los sistemas operativos.
- Incorporación de dispositivos.
- Administración del acceso.
- Creación y administración de roles para el control de acceso basado en roles.
- Configuración de los grupos de dispositivos.
- Configuración de las características avanzadas del entorno.

- **Al final de este módulo, podrá hacer lo siguiente:**
- Creación de un entorno de Microsoft Defender para punto de conexión
- Incorporación de dispositivos que Microsoft Defender para punto de conexión debe supervisar
- Configuración de Microsoft Defender para punto de conexión

## Módulo 13: Protección contra ataques malintencionados y accesos no autorizados con Microsoft Edge.

Microsoft Edge ayuda a proteger la red y los dispositivos frente a ataques malintencionados y ayuda a evitar el acceso no autorizado a los datos corporativos con SmartScreen de Microsoft Defender y Protección de aplicaciones de Microsoft Defender.

- Comprender las bases seguras de Microsoft Edge.
- Interceptar ataques malintencionados con SmartScreen de Microsoft Defender.
- Mejora de la seguridad del explorador con Protección de aplicaciones de Microsoft Defender.
- Administre controles y directivas para Microsoft Edge en Microsoft Endpoint Manager.

**Al final de este módulo, podrá:**

- Describir cómo se crea Microsoft Edge para una exploración segura.
- Usar SmartScreen de Microsoft Defender y Protección de aplicaciones para protegerse frente a ataques malintencionados y accesos no autorizados.
- Administrar las opciones de seguridad de Microsoft Edge a través de directivas y controles en Microsoft Endpoint Manager.

## Módulo 14: Descripción del cifrado Microsoft 365.

Obtenga información sobre cómo Microsoft 365 cifra los datos en reposo y en tránsito, administra de forma segura las claves de cifrado y proporciona opciones de administración de claves a los clientes para satisfacer sus necesidades empresariales y obligaciones de cumplimiento.

- Introducción al cifrado de Microsoft 365.
- Obtenga información sobre cómo BitLocker cifra los datos en reposo.
- Descripción del cifrado de servicio en Microsoft Purview.
- Explorar la administración de claves de cliente mediante la clave de cliente.
- Obtenga información sobre cómo se cifran los datos en tránsito.
- Comprobación de conocimiento y Resumen.

**Una vez completado este módulo, debería ser capaz de:**

- Explicar cómo el cifrado mitiga el riesgo de divulgación de datos no autorizados.
- Describir las soluciones de cifrado de datos en reposo y datos en tránsito de Microsoft.
- Explicar cómo Microsoft 365 implementa el cifrado de servicio para proteger los datos de los clientes en el nivel de aplicación.
- Comprender las diferencias entre las claves administradas por Microsoft y las claves administradas por el cliente para su uso con el cifrado de servicio.

## Módulo 15: Información sobre la administración de aplicaciones con Microsoft Intune.

Microsoft Intune ayuda a configurar aplicaciones, a proteger los datos de las aplicaciones, a administrar las asignaciones de directivas de aplicaciones y a poner en marcha reglas de seguridad de aplicaciones.

- Introducción.
- Descripción del ciclo de vida de la administración de aplicaciones.
- Configuración de aplicaciones.
- Protección de aplicaciones.
- Aplicaciones protegidas.
- Aplicación del marco de protección de datos.

**En este módulo, aprenderá a:**

- Configurar y proteger las aplicaciones de la organización.
- Describir el ciclo de vida de la administración de aplicaciones
- Aplicar el marco de protección de datos usando directivas de protección de aplicaciones

## Módulo 16: Administrar el cumplimiento de los dispositivos.

En este módulo, se examinan las directivas de cumplimiento de dispositivos, cómo las organizaciones las usan de forma eficaz,

cómo crear directivas y configurar usuarios y grupos condicionales, cómo crear directivas de acceso condicional y cómo supervisar los dispositivos inscritos.

- Introducción.
- Planear el cumplimiento de dispositivos.
- Implementación de directivas de cumplimiento para Intune dispositivos administrados.
- Supervisión de los resultados de las directivas de cumplimiento de dispositivos de Intune.
- Implementación de grupos de usuarios y dispositivos para supervisar el cumplimiento de dispositivos.
- Exploración de directivas de acceso condicional.
- Compilación de directivas de acceso condicional.
- Supervisar los dispositivos inscritos.

**Al final de este módulo, podrá:**

- Planee el cumplimiento del dispositivo definiendo las reglas y las opciones que deben configurarse en un dispositivo para que se considere compatible.
- Configure usuarios y grupos condicionales para implementar perfiles, directivas y aplicaciones.
- Cree directivas de acceso condicional para implementar decisiones automatizadas de control de acceso para acceder a sus aplicaciones en la nube.
- Supervise los dispositivos inscritos para controlar sus actividades de Intune y el estado de cumplimiento.

## Módulo 17: Remediar los riesgos con Microsoft Defender para Office 365.

Aprende sobre el componente Microsoft Defender para Office 365 de Microsoft 365 Defender.

- Introducción a Microsoft Defender para Office 365.
- Automatizar, investigar y remediar.
- Configurar, proteger y detectar.
- Simular ataques.

**En este módulo, aprenderás a:**

- Defina las capacidades de Microsoft Defender para Office 365.
- Comprende cómo simular ataques dentro de tu red.
- Explique cómo Microsoft Defender para Office 365 puede remediar los riesgos en su entorno.

## Módulo 18: Consulta, visualización y supervisión de datos en Microsoft Sentinel.

En este módulo se describe cómo consultar, visualizar y supervisar datos en Microsoft Sentinel.

- Supervisión y visualización de datos.
- Consulta de datos mediante el lenguaje de consulta Kusto.
- Uso de libros predeterminados de Microsoft Sentinel.
- Creación de un libro de Microsoft Sentinel.

**Ejercicios:**

- Consulta y visualización de datos con libros de Microsoft Sentinel.
- Visualización de datos mediante libros de Microsoft Sentinel.

**Objetivos de este módulo:**

- Visualizar datos de seguridad con libros de Microsoft Sentinel.
- Comprender cómo funcionan las consultas.
- Explorar las funciones de los libros.
- Crear un libro de Microsoft Sentinel.

## Módulo 19: Creación y administración de tipos de información confidencial.

Obtenga información sobre cómo usar tipos de información confidencial para respaldar su estrategia de protección de la información.

- Comparación de tipos de información confidencial integrados y personalizados.
- Creación y administración de tipos de información confidencial personalizados.
- Descripción de tipos de información confidencial personalizados con coincidencia exacta de datos.
- Implementar huellas digitales de documentos.
- Creación de un diccionario de palabras clave.

**Tras finalizar este módulo, podrá:**

- Reconocer la diferencia entre las etiquetas de confidencialidad integradas y personalizadas
- Configurar tipos de información confidencial con una clasificación exacta basada en coincidencias de datos
- Implementar huellas digitales de documentos
- Crear diccionarios de palabras clave personalizadas

## Módulo 20: Aplicación y administración de las etiquetas de confidencialidad.

Obtenga información sobre cómo se utilizan las etiquetas de confidencialidad para clasificar y proteger los datos empresariales, asegurándose de que la productividad de los usuarios y su capacidad de colaboración no se vean perjudicadas.

- Aplicación de etiquetas de confidencialidad en Microsoft Teams, grupos de Microsoft 365 y sitios de SharePoint.
- Planificación del etiquetado local.
- Configuración del etiquetado local para el analizador de etiquetado unificado.
- Aplicación de protecciones y restricciones al correo electrónico y a los archivos.
- Supervisión del rendimiento de las etiquetas mediante el análisis de etiquetas.

**Tras finalizar este módulo, podrá:**

- Aplicar etiquetas de confidencialidad con Microsoft Teams, grupos de Microsoft 365 y sitios de SharePoint.
- Supervisar el uso de etiquetas mediante el análisis de etiquetas.
- Configurar el etiquetado local.
- Administrar la configuración de protección y el marcado de las etiquetas de confidencialidad aplicadas.
- Aplicar protecciones y restricciones al correo electrónico.
- Aplicar protecciones y restricciones a los archivos.

## Módulo 21: Evitar la pérdida de datos en Microsoft Purview.

Aprenda a descubrir, clasificar y proteger el contenido sensible y crítico para el negocio a lo largo de su ciclo de vida en toda su organización.

- Resumen de la prevención de pérdidas de datos.
- Identificar el contenido para proteger.
- Defina la configuración de la política para su política de DLP.
- Pruebe y cree su política de DLP.
- Preparar el punto final DLP.
- Administrar alertas DLP en el portal de cumplimiento de Microsoft Purview.
- Ver informes de prevención de pérdida de datos.
- Implementar la extensión de Microsoft Purview.

**Cuando termines con este módulo, podrás:**

- Discuta la solución de prevención de pérdida de datos y sus beneficios.
- Describa el proceso de configuración de prevención de pérdida de datos.
- Explique lo que experimentarán los usuarios cuando se implemente la solución.

## Módulo 22: Administración de informes y directivas de prevención de pérdida de datos en Microsoft 365.

Obtenga información sobre cómo administrar directivas de prevención de pérdida de datos y mitigar las infracciones de la directiva de prevención de pérdida de datos.

- Configuración de la prevención de pérdida de datos para la prioridad de directivas.
- Implementación de directivas de prevención de pérdida de datos en modo de prueba.
- Explicación de las funcionalidades de los informes de prevención de pérdida de datos.
- Revisión y análisis de los informes de prevención de pérdida de datos.
- Administración de permisos en los informes de prevención de pérdida de datos.
- Administración y respuesta a infracciones de la directiva de prevención de pérdida de datos.

**Tras finalizar este módulo, podrá:**

- Revisar y analizar informes de DLP.
- Administrar permisos para informes de DLP.
- Identificar y mitigar las infracciones de las directivas DLP.
- Mitigación de las infracciones de DLP en Microsoft Defender for Cloud Apps.

## Módulo 23: Gestionar el ciclo de vida de los datos en Microsoft Purview.

Aprenda a administrar el ciclo de vida de su contenido utilizando soluciones para importar, almacenar y clasificar datos críticos para el negocio para que pueda conservar lo que necesita y eliminar lo que no necesita.

- Descripción general de la gestión del ciclo de vida de los datos.
- Configurar las políticas de retención.
- Configurar etiquetas de retención.
- Configurar políticas de etiquetas de retención manual.
- Configurar las políticas de etiquetas de retención de aplicación automática.
- Importar datos para la gestión del ciclo de vida de los datos.
- Gestionar, supervisar y remediar la gestión del ciclo de vida de los datos.

**Al completar este módulo, deberías ser capaz de:**

- Discuta la solución de gestión del ciclo de vida de los datos y sus beneficios.
- Enumere los escenarios de clientes a los que se dirige la solución de gestión del ciclo de vida de los datos.
- Describa el proceso de configuración de la gestión del ciclo de vida de los datos.
- Explique lo que experimentarán los usuarios cuando se implemente la solución.
- Articular las mejores prácticas de implementación y adopción.

## Módulo 24: Administración de la retención de datos en cargas de trabajo de Microsoft 365.

Aprenda a administrar la retención de Microsoft 365 y a implementan las soluciones de retención en los servicios de Microsoft 365 individuales.

- Introducción.
- Explicación de la retención en Exchange Online.
- Explicación de la retención en SharePoint Online y OneDrive.
- Explicación de la retención en Microsoft Teams.
- Explicación de la retención en Microsoft Yammer.
- Recuperación de contenido en cargas de trabajo de Microsoft 365.
- Activar buzones de archivo en Microsoft Exchange.
- Aplicación de la retención de buzones en Microsoft Exchange.
- Recuperación de contenido en Microsoft Exchange.

**Tras finalizar este módulo, podrá:**

- Describir las características de retención en cargas de trabajo de Microsoft 365.
- Configurar las opciones de retención en Microsoft Teams, Yammer y SharePoint Online.
- Recuperar contenido protegido por la configuración de retención.
- Recuperar elementos protegidos desde buzones de Exchange.

## Módulo 25: Administrar registros en Microsoft Purview.

Aprenda a usar la clasificación inteligente para automatizar y simplificar el programa de retención de registros regulatorios, legales y críticos para el negocio en su organización.

- Descripción general de la gestión de registros.
- Importar un plan de archivos.
- Configurar etiquetas de retención.
- Configurar la retención basada en eventos.
- Gestionar, supervisar y corregir registros.

**Al completar este módulo, deberías ser capaz de:**

- Discuta la solución de gestión de registros de Microsoft Purview y sus beneficios.
- Enumere los escenarios de clientes a los que se dirige la solución de gestión de registros de Microsoft.
- Describa el proceso de configuración de Microsoft Purview Records Management.
- Explique lo que experimentarán los usuarios cuando se implemente la solución.
- Articular las mejores prácticas de implementación y adopción.

## Módulo 26: Administrar cumplimiento en Microsoft 365 y Exchange Online.

Obtenga más información sobre cómo funciona el cumplimiento en un entorno de Exchange Online. Obtenga más información sobre cómo usar las directivas de retención y prevención de pérdida de datos para conservar los datos y las comunicaciones que necesita mantener. Asimismo, descubrirá cómo buscar datos y comunicaciones, y cómo asegurarse de que está listo para una auditoría.

- Introducción a la administración de cumplimiento.
- Configurar directivas de retención.
- Configurar la directiva de prevención de pérdida de datos.
- Configurar y analizar registros de auditoría.
- Administrar reglas del diario.
- Administrar búsqueda de contenido.

**Al final de este módulo, podrá hacer lo siguiente:**

- Explicar las directivas de retención.
- Explicar las directivas de prevención de pérdida de datos.
- Explicar los registros de auditoría.
- Explicar la búsqueda de contenido.

## Módulo 27: Administrar Microsoft Purview eDiscovery (Premium).

Este módulo explora cómo usar Microsoft Purview eDiscovery (Premium) para preservar, recopilar, analizar, revisar y exportar contenido que responda a las investigaciones internas y externas de una organización, y comunicarse con los custodios involucrados en un caso.

- Explora Microsoft Purview eDiscovery (Premium).
- Implementar Microsoft Purview eDiscovery (Premium).
- Crear y gestionar un caso de eDiscovery (Premium).
- Gestionar los custodios y las fuentes de datos no privativas de la custodia.
- Analizar el contenido del caso.

**Al final de este módulo, podrás:**

- Describe cómo Microsoft Purview eDiscovery (Premium) se basa en eDiscovery (Estándar).
- Describir el flujo de trabajo básico de eDiscovery (Premium).
- Crear y gestionar casos en eDiscovery (Premium).
- Administrar custodios y fuentes de datos sin custodia.
- Analice el contenido del caso y utilice herramientas analíticas para reducir el tamaño de los conjuntos de resultados de búsqueda.

## Módulo 28: Administre los requisitos regulatorios y de privacidad con Microsoft Priva.

Aprende a usar Microsoft Priva para gestionar las políticas de riesgo de privacidad y las solicitudes de derechos de sujeto.

- Crear y gestionar políticas de gestión de riesgos.
- Investigar y remediar las alertas de gestión de riesgos.
- Crear solicitudes de derechos.
- Gestionar la estimación y recuperación de datos para las solicitudes de derechos.
- Revisar los datos de las solicitudes de derechos.
- Obtener informes de solicitudes de derechos.

**Al completar este módulo, el alumno podrá:**

- Crear y gestionar políticas de gestión de riesgos para la sobreexposición de datos, la transferencia de datos y la minimización de datos
- Investigar y remediar las alertas de riesgo
- Enviar notificaciones al usuario
- Crear y gestionar solicitudes de derechos de sujeto
- Estimar y recuperar los datos del sujeto
- Revisar los datos del tema
- Crear informes de derechos temáticos

## Módulo 29: Preparar el cumplimiento de comunicaciones de Microsoft Purview.

Cumplimiento de comunicaciones en Microsoft Purview es una solución que ayuda a las organizaciones a abordar las infracciones de directivas de código de conducta en las comunicaciones de la compañía, mientras ayuda a las organizaciones en los sectores regulados a cumplir requisitos específicos de cumplimiento de supervisión. El Cumplimiento de comunicaciones usa el aprendizaje automático para detectar de forma inteligente las infracciones en los diferentes canales de comunicación, como Microsoft Teams, Exchange Online o mensajes de Yammer.

- Introducción al Cumplimiento de comunicaciones.
- Identificar y resolver el flujo de trabajo de cumplimiento de comunicaciones.
- Introducción a las directivas de Cumplimiento de comunicaciones.
- Investigar y corregir las alertas de cumplimiento de las comunicaciones.

**Caso práctico:**

- Configurar una directiva de lenguaje ofensivo.

**Una vez completado este módulo, debería poder:**

- Enumerar las mejoras en el cumplimiento de comunicaciones en relación con las directivas de supervisión de Office 365 que reemplazarán.
- Explicar cómo identificar y corregir las infracciones de directivas de código de conducta.
- Enumerar los requisitos previos que deben cumplirse antes de crear directivas de cumplimiento de comunicación.
- Describir los tipos de plantillas de directiva predefinidas e integradas.

## Módulo 30: Gestionar el riesgo interno en Microsoft Purview.

Microsoft Purview Insider Risk Management ayuda a las organizaciones a abordar los riesgos internos, como el robo de IP, el fraude y el sabotaje. Aprenda sobre la gestión de riesgos internos y cómo las tecnologías de Microsoft pueden ayudarle a detectar, investigar y tomar medidas sobre las actividades de riesgo en su organización.

- Visión general de la gestión de riesgos internos.
- Introducción a la gestión de políticas de riesgo interno.
- Crear y gestionar políticas de riesgo de información privilegiada
- Investigar las alertas de riesgo de información privilegiada.
- Tomar medidas sobre las alertas de riesgos internos a través de los casos.

**Al completar este módulo, deberías ser capaz de:**

- Explique cómo Microsoft Purview Insider Risk Management puede ayudar a prevenir, detectar y contener los riesgos internos en una organización.
- Describa los tipos de plantillas de políticas integradas y predefinidas.
- Enumere los requisitos previos que deben cumplirse antes de crear políticas de riesgo interno.
- Explique los tipos de acciones que puede tomar en un caso de gestión de riesgos internos.

## Módulo 31: Planear las barreras de información.

Las barreras de información permiten a los administradores definir directivas que permitan o impidan la comunicación entre grupos de usuarios en chats y canales de Microsoft Teams. Cuando haya directivas de barreras de información, las personas que no deberían comunicarse con otros usuarios específicos no podrán encontrar, seleccionar, chatear o llamar a esos usuarios. Con las barreras de información, se realizan comprobaciones para evitar comunicaciones no autorizadas.

- Introducción a la planificación de las barreras de información.
- Planear las barreras de información.
- Escenario de ejemplo sobre las barreras de información.

**Una vez completado este módulo, debería poder:**

- Describir cómo las directivas de barrera de información pueden ayudar a su organización a mantener el cumplimiento con normas y reglamentos relevantes del sector y evitar posibles conflictos de interés.
- Enumerar los tipos de situaciones en las que se podrían aplicar las barreras de información.
- Explicar el proceso de crear una directiva de barrera de información.
- Explicar cómo solucionar problemas inesperados haya barreras de información aplicadas.

## Módulo 32: Implementar administración de acceso con privilegios.

La administración de acceso con privilegios permite un control de acceso granular sobre las tareas de administración con privilegios en Office 365. La administración de acceso con privilegios requiere que los usuarios que deben llevar a cabo tareas con privilegios o privilegios elevados soliciten el acceso de forma puntual a través de un flujo de trabajo de aprobación muy limitado en cuanto al ámbito y al tiempo. Esta configuración proporciona a los usuarios el acceso suficiente para realizar la tarea que deban realizar sin arriesgarse a la exposición de datos confidenciales o la configuración crítica.

- Introducción a la administración de acceso e identidades.

**Caso práctico:**

- Implementar una administración de acceso con privilegios.

**Una vez completado este módulo, debería poder:**

- Explicar la diferencia entre la administración de acceso con privilegios y la administración de identidades con privilegios.
- Describir el flujo del proceso de administración del acceso con privilegios.
- Describir cómo configurar y habilitar la administración de acceso con privilegios.

## Módulo 33: Administrar la Caja de seguridad del cliente.

La Caja de seguridad del cliente admite solicitudes de acceso a datos en Exchange Online, SharePoint Online y OneDrive cuando los ingenieros de Microsoft necesitan tener acceso al contenido del cliente para determinar la causa raíz de un problema y corregirlo. La Caja de seguridad del cliente requiere que el ingeniero solicite acceso al cliente como un último paso en el

flujo de trabajo de aprobación. Esto permite a las organizaciones aprobar o rechazar estas solicitudes y proporcionar un control de acceso directo al cliente.

- Introducción a Caja de seguridad del cliente.
- Administrar solicitudes de Caja de seguridad del cliente.

**Una vez completado este módulo, debería poder:**

- Describir el flujo de trabajo de Caja de seguridad del cliente.
- Aprobar o denegar una solicitud de Caja de seguridad del cliente
- Explicar cómo puede auditar las acciones que realizan los ingenieros de Microsoft cuando se aprueban las solicitudes de acceso.